

Beschreibung

Verfahren zum Zugriff auf eine Datenverarbeitungsanlage

- 5 Die Erfindung betrifft ein Verfahren zum Zugriff auf eine Datenverarbeitungsanlage.

- Nach dem Stand der Technik sind weithin Datenverarbeitungsanlagen bekannt, die aus einer Mehrzahl
10 miteinander zum Datenaustausch vernetzter Datenverarbeitungseinheiten, z. B. Personalcomputer, computergesteuerte Geräte, Server und dgl., bestehen. Dabei ist jeder Datenverarbeitungseinheit eine beschränkte Zahl von Benutzern zugewiesen. Um eine unbefugte Benutzung einer
15 Datenverarbeitungseinheit zu unterbinden, verfügt jeder Benutzer über ein persönliches Passwort. Durch Eingeben des Passworts authentifiziert sich der Benutzer und erhält Zugriff auf die Datenverarbeitungsanlage.
- 20 Insbesondere in Krankenhäusern sind Datenverarbeitungsanlagen heute komplex aufgebaut. Bestandteil solcher Datenverarbeitungsanlagen sind u. a. Diagnose- und Analysegeräte. Derartige Geräte müssen stets in einem einwandfreien Funktionszustand gehalten werden. Insbesondere
25 eine Wartung und eine Reparatur derartiger Geräte erfordert in der Regel einen Zugriff eines Systemtechnikers auf die Datenverarbeitungsanlage. Ein nach wie vor ungelöstes Problem dabei ist, dass damit der Systemtechniker u. U. Zugriff auf personenbezogene Patientendaten erhalten kann. Aus
30 datenschutzrechtlichen Gründen darf ein Zugriff auf eine solche Datenverarbeitungsanlage nur nach dem 4-Augen-Prinzip erfolgen, d. h. nur gleichzeitig durch zwei befugte Personen. In der Praxis lässt sich das allerdings kaum realisieren, weil im Falle einer Funktionsstörung einer
35 Datenverarbeitungsanlage in der Regel eine sofortige Abhilfe erforderlich ist und mitunter zwei befugte und zur Behebung

der Funktionsstörung ausreichend qualifizierte Systemtechniker nicht immer gleichzeitig verfügbar sind.

Aus der **DE 101 21 819 A1** ist ein Verfahren bekannt, bei dem ein Arzt nur dann Zugriff auf patientenspezifische Daten erhält, wenn der Arzt eine ihm zugewiesene erste Chip-Karte und der gleichzeitig anwesende Patient eine ihm gehörende zweite Chip-Karte in eine beim Arzt befindliche Datenverarbeitungseinrichtung zur Authentifizierung einlesen.

Aufgabe der Erfindung ist es, ein Verfahren anzugeben, welches einen eine Datenhoheit eines Systemadministrators sicherstellenden Zugriff auf eine Datenverarbeitungsanlage lediglich nach dem Grundsatz des 4-Augen-Prinzips ermöglicht.

Diese Aufgabe wird durch die Merkmale des Anspruchs 1 gelöst. Zweckmäßige Ausgestaltungen des Verfahrens ergeben sich aus den Merkmalen der Ansprüche 2 bis 13.

Nach Maßgabe der Erfindung ist ein Verfahren zum Zugriff auf eine Datenverarbeitungsanlage vorgesehen, welche aus miteinander zum Datenaustausch vernetzten Datenverarbeitungseinheiten gebildet ist, mit folgenden Schritten:

Bereitstellen eines ersten Authentifizierungsmittels zur Authentifizierung eines Systemadministrators,

Authentifizierung des Systemadministrators an einer ersten Datenverarbeitungseinheit durch Übergabe des ersten Authentifizierungsmittels an ein Authentifizierungsprogramm,

Bereitstellen eines zweiten Authentifizierungsmittels zur Authentifizierung eines Systemtechnikers,

Authentifizierung des Systemtechnikers an einer zweiten Datenverarbeitungseinheit durch Übergabe des zweiten

Authentifizierungsmittels an das Authentifizierungsprogramm, und dadurch bedingtes automatisches Erzeugen einer den Träger des zweiten Authentifizierungsmittels identifizierenden Identifikationsinformation,

5

Anzeige der Identifikationsinformation an der ersten Datenverarbeitungseinheit (1) des Systemadministrators und

10 Freischalten einer Zugangsberechtigung für den Systemtechniker und bedingtes automatisches Auslösen einer Funktion zum Erzeugen und Speichern einer die Tätigkeit des Systemtechnikers an der Datenverarbeitungsanlage protokollierenden Protokolldatei.

15 Nach dem erfindungsgemäßen Verfahren erhält der Systemtechniker erst nach Übergabe eines ihm zugewiesenen zweiten Authentifizierungsmittels Zugang zur Datenverarbeitungsanlage. Die Freischaltung eines solchen Zugangs wird durch das Erzeugen einer

20 Identifizierungsinformation dokumentiert und an der ersten Datenverarbeitungseinheit des Systemadministrators angezeigt. Es wird außerdem eine die Tätigkeit des Systemtechnikers protokollierende Protokolldatei erzeugt, anhand derer der Eingriff des Systemtechnikers beispielsweise

25 für den Systemadministrator nachvollzogen werden kann. Damit ist gewährleistet, dass die Datenhoheit stets der Systemadministrator inne hat. Anhand der erzeugten Protokolldateien ist es ihm möglich zu prüfen, ob ein Systemtechniker unbefugterweise auf Daten zugegriffen hat. In

30 diesem Fall kann der Systemadministrator sofort jeglichen weiteren Zugang zur Datenverarbeitungsanlage für den betreffenden Systemtechniker sperren. Mit dem vorgeschlagenen Verfahren wird ein Zugriff auf eine Datenverarbeitungsanlage nach dem Grundsatz des 4-Augen-Prinzips ermöglicht. Dabei ist

35 es von besonderem Vorteil, dass ein solcher Zugriff auch dann erfolgen kann, wenn mit Kenntnis des Systemadministrators

lediglich ein Systemtechniker an einer
Datenverarbeitungseinheit tätig ist.

Unter dem Begriff "Zugriff" wird im Sinne der vorliegenden
5 Erfindung jegliche Tätigkeit verstanden, bei welcher der
Datenbestand einer Datenverarbeitungsanlage gesichtet,
verändert oder ganz oder teilweise kopiert wird. Bei einer
"Datenverarbeitungseinheit" im Sinne der vorliegenden
10 Erfindung handelt es sich um eine Vorrichtung, welche mit
anderen zum Datenaustausch geeigneten Vorrichtungen zum
Datenaustausch verbunden ist. Derartige Vorrichtungen weisen
zum Datenaustausch üblicherweise eine bidirektionale
Schnittstelle auf. Es kann sich dabei um einen
15 Personalcomputer, um computergesteuerte Anlagen oder Geräte
und dgl. handeln.

Unter dem Begriff "Systemadministrator" wird eine Person
verstanden, welche besondere Rechte im Hinblick auf die
Pflege und Wartung der Datenverarbeitungsanlage hat. Der
20 Systemadministrator im Sinne der vorliegenden Erfindung hat
im Gegensatz zu einem Systemtechniker die Möglichkeit, einen
Zugang zur Datenverarbeitungsanlage zu gestatten oder zu
sperren. Diese Möglichkeit wird dem Systemadministrator
insbesondere durch das erste Authentifizierungsmittel
25 zugewiesen.

Zur Authentifizierung des Systemtechnikers kann das zweite
Authentifizierungsmittel mittels des
Authentifizierungsprogramms durch Zugriff auf eine
30 verifizierte zweite Authentifizierungsmittel enthaltende
Datei verglichen und bei Übereinstimmung mit einem der
verifizierten zweiten Authentifizierungsmittel eine
entsprechende Information an den Systemadministrator
übermittelt werden. Unter einem "verifizierten zweiten
35 Authentifizierungsmittel" wird eine Kopie des an den
Systemtechnikers übergebenen zweiten
Authentifizierungsmittels verstanden, welche vom

Systemadministrator in einer nur ihm zugänglichen Datei verwaltet wird. Zum Zugriff auf die Datenverarbeitungsanlage übergibt der Systemadministrator an jeden Systemtechniker ein besonderes zweites Authentifizierungsmittel. Zur

- 5 Erleichterung der Prüfung der Authentizität der zweiten Authentifizierungsmittel werden diese gemeinsam in der Datei abgelegt. Sofern das Authentifizierungsprogramm feststellt, dass eine Zugriffsanforderung auf der Grundlage eines mit einem verifizierten zweiten Authentifizierungsmittel
10 identischen zweiten Authentifizierungsmittels vorliegt, wird dem Systemadministrator das anhand einer geeigneten Information angezeigt. Vorteilhafterweise ist jedem in der Datei enthaltenen verifizierten zweiten Authentifizierungsmittel eine dafür spezifische
15 Identifikationsinformation zugeordnet. Es kann sich dabei beispielsweise um den Namen und ggf. die Zugehörigkeit des Systemtechnikers zu einer bestimmten Organisation handeln. Im Falle einer Übereinstimmung des zweiten Authentifizierungsmittels mit einem der in der Datei
20 hinterlegten verifizierten zweiten Authentifizierungsmittel können dem Systemadministrator also zusätzlich der Name und die Organisation des Systemtechnikers angezeigt werden.

- In einem besonders einfachen Fall handelt es sich beim ersten
25 und/oder zweiten Authentifizierungsmittel um einen, vorzugsweise mittels einer an einer Datenverarbeitungseinheit vorgesehenen Tastatur, an das Authentifizierungsprogramm übergebaren Authentifizierungscode. Zur Erhöhung der Sicherheit ist es zweckmäßig, dass der Authentifizierungscode
30 in einer mobilen, mit der Datenverarbeitungsanlage zur Datenübertragung verbindbaren Speichereinheit gespeichert ist. Bei der Speichereinheit kann es sich um eine mit einem Datenträger versehene Authentifizierungskarte handeln. Die Authentifizierungskarte kann ein Speichermittel, insbesondere
35 zum Speichern der Protokolldatei und/oder eine den Zugriff auf die Protokolldatei ermöglichenden Information, aufweisen. Bei der Information kann es sich beispielsweise um einen

"Link" handeln, anhand dessen die Protokolldatei aufgefunden und geöffnet werden kann.

5 Zur Erhöhung der Sicherheit kann das Freischalten einer
Zugangsberechtigung durch den Systemadministrator durch
manuelles Auslösen einem im Authentifizierungsprogramm dafür
vorgesehenen und ausschließlich dem Systemadministrator
zugänglichen Funktion erfolgen. Damit ist sichergestellt,
10 dass ein Zugriff nur mit aktiver Zustimmung des
Systemadministrators erfolgt. Es kann aber auch sein, dass
der Zugriff nach einer automatischen Prüfung des zweiten
Authentifizierungsmittels dem Systemtechniker automatisch
eingeräumt wird. Auch in diesem Fall wird erfindungsgemäß
15 automatisch insbesondere eine Protokolldatei erstellt. Das
ermöglicht einen Zugriff auf Datenverarbeitungsanlagen,
insbesondere in Krankenhäusern, die ununterbrochen
funktionsbereit gehalten werden müssen.

20 Nach einer weiteren Ausgestaltung ist vorgesehen, dass die
Verbindung zwischen der ersten und der zweiten
Datenverarbeitungseinheit über das Internet oder ein Intranet
hergestellt wird. Das ermöglicht einen Zugriff des
Systemtechnikers von einer entfernt vorgesehenen zweiten
Datenverarbeitungseinheit. Es ist somit möglich, dass ein für
25 die jeweilige Problemstellung optimal qualifizierter
Systemtechniker jederzeit, d. h. unabhängig von seinem
Aufenthaltsort, auf die Datenverarbeitungsanlage zugreifen
kann. Das ermöglicht eine schnelle und effektive Beseitigung
von Funktionsstörungen. Gleichzeitig wird dabei die
30 Authentizität des zugreifenden Systemtechnikers
sichergestellt und dessen Tätigkeit protokolliert. Der
Zugriff des Systemtechnikers erfolgt auch in diesem Fall nach
dem Grundsatz des 4-Augen-Prinzips. Mittels der
Datenverarbeitungsanlage werden insbesondere Daten
35 verarbeitet, welche einer einzelnen Person nur mit besonderer
Berechtigung oder bei Nichtvorliegen der besonderen
Berechtigung nur Personen mit einer einfachen Berechtigung

nach dem 4-Augen-Prinzip zugänglich gemacht werden dürfen.
Die besondere Berechtigung wird zweckmäßigerweise durch
Übergabe eines der Person zugewiesenen dritten
Authentifizierungsmittels an die Datenverarbeitungsanlage
5 nachgewiesen. Bei der einzelnen Person mit besonderer
Berechtigung kann es sich beispielsweise um einen Arzt
handeln. Bei den Daten kann es sich um schutzbedürftige
personenbezogene Daten, insbesondere Patientendaten, handeln.

10 Nachfolgend wird ein Ausführungsbeispiel der Erfindung anhand
der Zeichnung näher erläutert. Es zeigen:

Fig. 1 das Verfahren anhand einer schematischen Übersicht
und

15

Fig. 2 die wesentlichen Bestandteile eines
Authentifizierungsprogramms.

Fig. 1 zeigt schematisch eine erste Datenverarbeitungseinheit
20 1, z. B. einen Personalcomputer. Die erste
Datenverarbeitungseinheit 1 ist Bestandteil einer ersten
vernetzten Datenverarbeitungsanlage D1, welche als weitere
Datenverarbeitungseinheiten z. B. computergesteuerte Geräte 2
oder weitere Personalcomputer 3 umfasst. Die erste
25 Datenverarbeitungseinheit 1 ist einem Systemadministrator 4
zugewiesen, der die Datenhoheit über die erste
Datenverarbeitungsanlage D1 inne hat. Der Systemadministrator
4 ist insbesondere dazu berechtigt, mittels eines ersten
Programms 5 Benutzern der ersten Datenverarbeitungsanlage D1
30 Rollen und Rechte zuzuweisen. Derartige Rollen und Rechte
ermöglichen dem jeweiligen Benutzer lediglich Zugang zu den
für seinen Arbeitsbereich notwendigen Daten. Die Benutzer
können auf solchen Daten jederzeit Zugreifen, d. h. auch wenn
der Systemadministrator 4 nicht in die erste
35 Datenverarbeitungsanlage D1 eingeloggt ist.

Die erste Datenverarbeitungsanlage D1 ist über eine mit einer Firewall 6 gesicherte Datenleitung 7 mit einer zweiten Datenverarbeitungsanlage D2 einer Serviceorganisation verbunden. Die Verbindung kann beispielsweise über das Internet oder ein Intranet hergestellt werden. Die zweite Datenverarbeitungsanlage D2 umfasst eine zweite Datenverarbeitungseinheit 7, z. B. einen Personalcomputer, die einem Systemtechniker 8 zugewiesen ist.

Der Systemadministrator 4 besitzt zu seiner Authentifizierung eine erste Speicherkarte 9, auf der ein erster Authentifizierungscode gespeichert ist. Der erste Authentifizierungscode kann mittels eines geeigneten Lesegeräts der ersten Datenverarbeitungsanlage D1 zum Auslesen bereitgestellt werden. Der Systemtechniker 8 besitzt zu seiner Authentifizierung eine zweite Speicherkarte 10, auf der ein zweiter Authentifizierungscode gespeichert ist. Mittels eines geeigneten Lesegeräts kann der zweite Authentifizierungscode ausgelesen und der ersten Datenverarbeitungsanlage D1 zugänglich gemacht werden. Die Leseinheit zum Auslesen der zweiten Speicherkarte 10 muss dabei nicht unbedingt Bestandteil der ersten Datenverarbeitungsanlage D1 sein. Sie kann auch Bestandteil der zweiten Datenverarbeitungsanlage D2 sein. In diesem Fall kann die Authentizität des zweiten Authentifizierungscodes mittels eines zweiten bei der zweiten Datenverarbeitungsanlage D2 vorgesehenen Programms 11 vor dem Versuch eines Zugriffs auf die erste Datenverarbeitungsanlage D1 geprüft werden.

Die Funktion der Vorrichtung ist folgende:

Zunächst schließen ein für die erste Datenverarbeitungsanlage D1 verantwortlicher IT-Manager 12 und eine Serviceorganisation bzw. der Systemtechniker 8 einen Servicevertrag ab. Nach Abschluss eines solchen Servicevertrags erhält der Systemtechniker 8 vom IT-Manager

12 eine zweite Speicherkarte 10, auf welcher der zweite Authentifizierungscode gespeichert ist.

Bei einem ersten Wartungs-/Reparaturfall fordert der System-
5 administrator 4 mittels Telefonanruf oder per E-Mail eine Serviceleistung vom Servicetechniker 8 ab. Dabei kann es sich um eine Serviceleistung handeln, die von der zweiten Datenverarbeitungseinheit 7 aus erledigt werden kann. In diesem Fall übergibt der Servicetechniker 8 die zweite
10 Speicherkarte 10 an ein bei der zweiten Datenverarbeitungseinheit 7 vorgesehenes Lesegerät. Infolgedessen wird der dem Servicetechniker 8 authentifizierende zweite Authentifizierungscode innerhalb der zweiten Datenverarbeitungsanlage D2 an das zweite
15 Programm 11 übermittelt. Der zweite Authentifizierungscode wird geprüft. Sofern das zweite Programm 11 den zweiten Authentifizierungscode als authentisch erkennt, wird über die Datenleitung 7 eine Verbindung zur ersten Datenverarbeitungsanlage D1 hergestellt. Mittels des ersten
20 Programms 5 wird der gewünschte Zugriff geprüft. Dazu wird zunächst geprüft, ob die erste Speicherkarte 9 in einem Lesegerät, z. B. bei der ersten Datenverarbeitungseinheit 1, eingesteckt ist. Sofern das nicht der Fall ist, wird ein Zugriff durch den Systemtechniker 8 nicht ermöglicht. Sofern
25 ein Zugriff auf den auf der ersten Speicherkarte 9 gespeicherten ersten Authentifizierungscode zur Authentifizierung des Systemadministrators 4 möglich ist, wird der zweite Authentifizierungscode mit einer Mehrzahl von in einer Datei gespeicherten zweiten Authentifizierungscodes
30 verglichen. Sofern der zweite Authentifizierungscode als nicht authentisch erkannt wird, wird ein Zugang für den Systemtechniker 8 nicht ermöglicht. Sofern der zweite Authentifizierungscode als authentisch erkannt wird, wird eine Protokollfunktion ausgelöst. Gleichzeitig erhält der
35 Systemtechniker 8 Zugriff auf die erste Datenverarbeitungsanlage D1. Solange der Servicetechniker 8 auf die erste Datenverarbeitungsanlage D1 zugreift, werden

sämtliche Änderungen, Ergänzungen und dgl. am Datenbestand der ersten Datenverarbeitungsanlage D1 protokolliert. Sobald der Systemtechniker 8 seine Tätigkeit abgeschlossen und sich ausgeloggt hat, wird die Protokolldatei geschlossen.

5

Die Protokolldatei enthält neben dem Protokoll über sämtliche Änderungen, Ergänzungen und dgl. am Datenbestand der ersten Datenverarbeitungsanlage D1 vorteilhafterweise zusätzlich die folgenden Informationen:

10

- Name des Systemtechnikers,

- Name der Serviceorganisation,

15

- Login-/Logout-Zeit,

- Art des Zugangs, ggf. Identifikation der zum Zugang verwendeten Datenverarbeitungseinheit.

20 Bei einem zweiten Wartungs-/Reparaturfall fordert der Systemadministrator mittels des Telefonanrufs oder per E-Mail eine Serviceleistung vom Servicetechniker 8 an, welche vor Ort auszuführen ist. Es kann sich dabei z. B. um einen Austausch eines Moduls bei einem Röntgen-Computertomografen in einem
25 Krankenhaus handeln. In diesem Fall loggt sich der Servicetechniker 8 an einer geeigneten Datenverarbeitungseinheit der ersten Datenverarbeitungsanlage D1 unter Verwendung der zweiten Speicherkarte 10 ein. Ein Zugriff ist auch in diesem Fall nur dann möglich, wenn
30 gleichzeitig der Systemadministrator 4 unter Verwendung der ersten Speicherkarte 9 bei der ersten Datenverarbeitungsanlage D1 eingeloggt ist.

35 Nach einer weiteren vorteilhaften Funktion kann der Systemadministrator 4 jederzeit die Tätigkeit des Systemtechnikers 8 unterbrechen, indem er einen Zugriff auf die erste Datenverarbeitungsanlage D1 durch Unterbrechung des

Zugriffs auf den ersten Authentifizierungscode unterbricht.
Das kann z. B. dadurch erfolgen, dass der Systemadministrator
4 die erste Speicherkarte 9 aus dem betreffenden Lesegerät
herausnimmt. Im Gegensatz zu herkömmlichen Verfahren behält
5 nach dem erfindungsgemäßen Verfahren der Systemadministrator
4 also stets die Datenhoheit. Außerdem ist es anhand der
automatischen Protokollierungsfunktion möglich, sämtliche
Tätigkeiten des Systemtechnikers 8 nachzuvollziehen. Im Falle
eines Missbrauchs kann ein weiterer Zugriff vom
10 Systemadministrator 8 auf die erste Datenverarbeitungsanlage
D1 ohne weiteres gesperrt werden. Dazu muss lediglich der in
der Datei gespeicherte betreffende zweite
Authentifizierungscode entfernt oder geändert werden.

15 Mit dem vorgeschlagenen Verfahren ist ein Zugriff des
Systemtechnikers 8 auf den Datenbestand der ersten
Datenverarbeitungsanlage D1 nur nach dem 4-Augen-Prinzip
möglich, d. h. ein solcher Zugriff erfolgt stets unter der
Kontrolle des Systemadministrators 4. Insoweit kann ein
20 unbefugter Zugriff des Systemtechnikers 8 auf
schutzbedürftige personenbezogene Daten, z. B.
Patientendaten, unterbunden werden.

Fig. 2 zeigt schematisch die wesentlichen Bestandteile des
25 ersten Programms 5. Mit UI1 ist eine erste
Benutzerschnittstelle zum Zugriff von der ersten
Datenverarbeitungsanlage D1 und mit UI2 eine zweite
Benutzerschnittstelle zum Zugriff z. B. über die Datenleitung
7 bezeichnet.

30 Ein Zugriffsmodul 13 ermöglicht oder sperrt einen Zugriff für
einen Systemtechniker 8 auf die erste
Datenverarbeitungsanlage D1. Das Zugriffsmodul 13 verwaltet
und vergleicht insbesondere Authentifizierungscodes.

35 Vorteilhafterweise kann das erste Programm 5 weitere Module
aufweisen, welche insbesondere Wartungs- und/oder

Reparaturarbeiten an der ersten Datenverarbeitungsanlage D1 erleichtern. So kann z. B. ein Lokalisierungsmodul 14 vorgesehen sein, mit dem festgestellt werden kann, an welcher Datenverarbeitungseinheit ein qualifizierter Systemtechniker 8 gerade tätig und ggf. abrufbar ist.

Mit dem Protokollierungsmodul 15 wird eine Protokollierung der Tätigkeit des Systemtechnikers 8 bewirkt. Mit dem Protokollierungsmodul 15 werden insbesondere Protokolldateien erstellt und an einem vorgegebenen Ort abgelegt.

Ein Anonymisierungsmodul 16 dient insbesondere dazu, schutzbedürftige persönliche Daten zu anonymisieren. So können z. B. Namen von Patienten durch Kennziffern ersetzt werden, um einen Systemtechniker 8 entsprechend den Datenschutzvorschriften einen Einblick in persönliche Daten unmöglich zu machen.

Mit Hilfsmodulen 17, 18 wird eine Beschreibung der für den Systemadministrator 4 und den Systemtechniker 8 notwendigen Funktionen des ersten Programms 5 bereitgestellt. Ein Modalitätsmodul 19 ermöglicht einen Datenaustausch, z. B. mit computergesteuerten Geräten, wie Röntgen-Computertomografen usw.. In ähnlicher Weise ermöglicht ein IT-Systemmodul 20 einen Datenaustausch mit Datenbanken etc.

Ein Betriebssystemmodul 21 schafft die notwendigen Voraussetzungen für eine korrekte Einbindung des ersten Programms 5 in das jeweils benutzte Betriebssystem.

Patentanspruch

1. Verfahren zum Zugriff auf eine Datenverarbeitungsanlage (D1), welche aus miteinander zum Datenaustausch vernetzten Datenverarbeitungseinheiten (1, 2, 3) gebildet ist, mit
5 folgenden Schritten:

Bereitstellen eines ersten Authentifizierungsmittels (9) zur Authentifizierung eines Systemadministrators (4),
10

Authentifizierung des Systemadministrators (4) an einer ersten Datenverarbeitungseinheit (1) durch Übergabe des ersten Authentifizierungsmittels (9) an ein Authentifizierungsprogramm (5),
15

Bereitstellen eines zweiten Authentifizierungsmittels (10) zur Authentifizierung eines Systemtechnikers (8),

Authentifizierung des Systemtechnikers (8) an einer zweiten Datenverarbeitungseinheit (7) durch Übergabe des zweiten Authentifizierungsmittels (10) an das Authentifizierungsprogramm (5) und dadurch bedingtes automatisches Erzeugen einer den Träger des zweiten Authentifizierungsmittels (10) identifizierenden Identifikationsinformation,
20
25

Anzeige der Identifikationsinformation an der ersten Datenverarbeitungseinheit (1) des Systemadministrators (4) und
30

Freischalten einer Zugangsberechtigung für den Systemtechniker (8) und automatisches Auslösen einer Funktion zum Erzeugen und Speichern einer die Tätigkeit des Systemtechnikers (8) an der Datenverarbeitungsanlage (D1) protokollierenden Protokolldatei.
35

2. Verfahren nach Anspruch 1, wobei das zweite Authentifizierungsmittel (10) mittels des Authentifizierungsprogramms (5) durch Zugriff auf eine verifizierte zweite Authentifizierungsmittel (10) enthaltende
- 5 Datei verglichen und bei Übereinstimmung mit einem der verifizierten zweiten Authentifizierungsmittel (10) eine entsprechende Information an den Systemadministrator (4) übermittelt wird.
- 10 3. Verfahren nach Anspruch 2, wobei jedem in der Datei enthaltenen verifizierten zweiten Authentifizierungsmittel (10) eine dafür spezifische Identifikationsinformation zugeordnet ist.
- 15 4. Verfahren nach Anspruch 3, wobei die Identifikationsinformation den Namen und ggf. die Zugehörigkeit des Systemtechnikers (8) zu einer bestimmten Organisation umfasst.
- 20 5. Verfahren zum Zugriff auf eine Datenverarbeitungsanlage (D1), welche aus miteinander zum Datenaustausch vernetzten Datenverarbeitungseinheiten (1, 2, 3) gebildet ist, mit folgenden Schritten:
- 25 Bereitstellen eines ersten Authentifizierungsmittels (9) zur Authentifizierung eines Systemadministrators (4),
- Authentifizierung des Systemadministrators (4) an einer ersten Datenverarbeitungseinheit (1) durch Übergabe des
- 30 ersten Authentifizierungsmittels (9) an ein Authentifizierungsprogramm (5),
- Bereitstellen eines zweiten Authentifizierungsmittels (10) zur Authentifizierung eines Systemtechnikers (8),
- 35 Authentifizierung des Systemtechnikers (8) an einer zweiten Datenverarbeitungseinheit (7) durch Übergabe des zweiten

Authentifizierungsmittels (10) an das
Authentifizierungsprogramm (5) und dadurch bedingtes
automatisches Erzeugen einer den Träger des zweiten
Authentifizierungsmittels (10) identifizierenden

5 Identifikationsinformation,

wobei das erste (9) und/oder das zweite
Authentifizierungsmittel (10) ein, vorzugsweise mittels einer
an einer Datenverarbeitungseinheit (1, 7) vorgesehenen
10 Tastatur, an das Authentifizierungsprogramm (5) übergebbarer
Authentifizierungscode ist,

Anzeige der Identifikationsinformation an der ersten
Datenverarbeitungseinheit (1) des Systemadministrators (4)
15 und

Freischalten einer Zugangsberechtigung für den
Systemtechniker (8) und automatisches Auslösen einer Funktion
zum Erzeugen und Speichern einer die Tätigkeit des
20 Systemtechnikers (8) an der Datenverarbeitungsanlage (D1)
protokollierenden Protokolldatei.

6. Verfahren nach Anspruch 5, wobei der
Authentifizierungscode in einer mobilen mit der
25 Datenverarbeitungsanlage (D1, D2) zur Datenübertragung
verbindbaren Speichereinheit gespeichert ist.

7. Verfahren nach Anspruch 6, wobei die Speichereinheit eine
mit einem Datenträger versehene Authentifizierungskarte (9,
30 10) ist.

8. Verfahren nach Anspruch 7, wobei die
Authentifizierungskarte (9, 10) ein Speichermittel,
insbesondere zum Speichern der Protokolldatei und/oder einer
35 den Zugriff auf die Protokolldatei ermöglichenden
Information, aufweist.

9. Verfahren zum Zugriff auf eine Datenverarbeitungsanlage (D1), welche aus miteinander zum Datenaustausch vernetzten Datenverarbeitungseinheiten (1, 2, 3) gebildet ist, mit folgenden Schritten:

5

Bereitstellen eines ersten Authentifizierungsmittels (9) zur Authentifizierung eines Systemadministrators (4),

10 Authentifizierung des Systemadministrators (4) an einer ersten Datenverarbeitungseinheit (1) durch Übergabe des ersten Authentifizierungsmittels (9) an ein Authentifizierungsprogramm (5),

15 Bereitstellen eines zweiten Authentifizierungsmittels (10) zur Authentifizierung eines Systemtechnikers (8),

20 Authentifizierung des Systemtechnikers (8) an einer zweiten Datenverarbeitungseinheit (7) durch Übergabe des zweiten Authentifizierungsmittels (10) an das Authentifizierungsprogramm (5) und dadurch bedingtes automatisches Erzeugen einer den Träger des zweiten Authentifizierungsmittels (10) identifizierenden Identifikationsinformation,

25 Anzeige der Identifikationsinformation an der ersten Datenverarbeitungseinheit (1) des Systemadministrators (4) und

30 Freischalten einer Zugangsberechtigung für den Systemtechniker (8) und automatisches Auslösen einer Funktion zum Erzeugen und Speichern einer die Tätigkeit des Systemtechnikers (8) an der Datenverarbeitungsanlage (D1) protokollierenden Protokolldatei,

35 wobei das Freischalten einer Zugangsberechtigung durch den Systemadministrator (4) durch manuelles Auslösen einer im Authentifizierungsprogramm (5) dafür vorgesehenen und

ausschließlich dem Systemadministrator (8) zugänglichen Funktion erfolgt.

10. Verfahren nach einem der vorhergehenden Ansprüche, wobei
5 mittels der Datenverarbeitungsanlage (D1) Daten verarbeitet werden, welche

einer einzelnen Person nur mit besonderer Berechtigung

10 oder

bei Nichtvorliegen der besonderen Berechtigung nur Personen mit einer einfachen Berechtigung nach dem 4-Augen-Prinzip

15 zugänglich gemacht werden dürfen.

11. Verfahren nach Anspruch 10, wobei die besondere Berechtigung durch Übergabe eines der Person zugewiesenen dritten Authentifizierungsmittels an die
20 Datenverarbeitungsanlage (D1) nachgewiesen wird.

12. Verfahren nach Anspruch 10, wobei die Daten schutzbedürftige personenbezogene Daten, insbesondere Patientendaten, sind.

25

13. Verfahren nach Anspruch 1, wobei die Verbindung zwischen der ersten (1) und der zweiten Datenverarbeitungseinheit (7) über das Internet oder ein Intranet hergestellt wird.

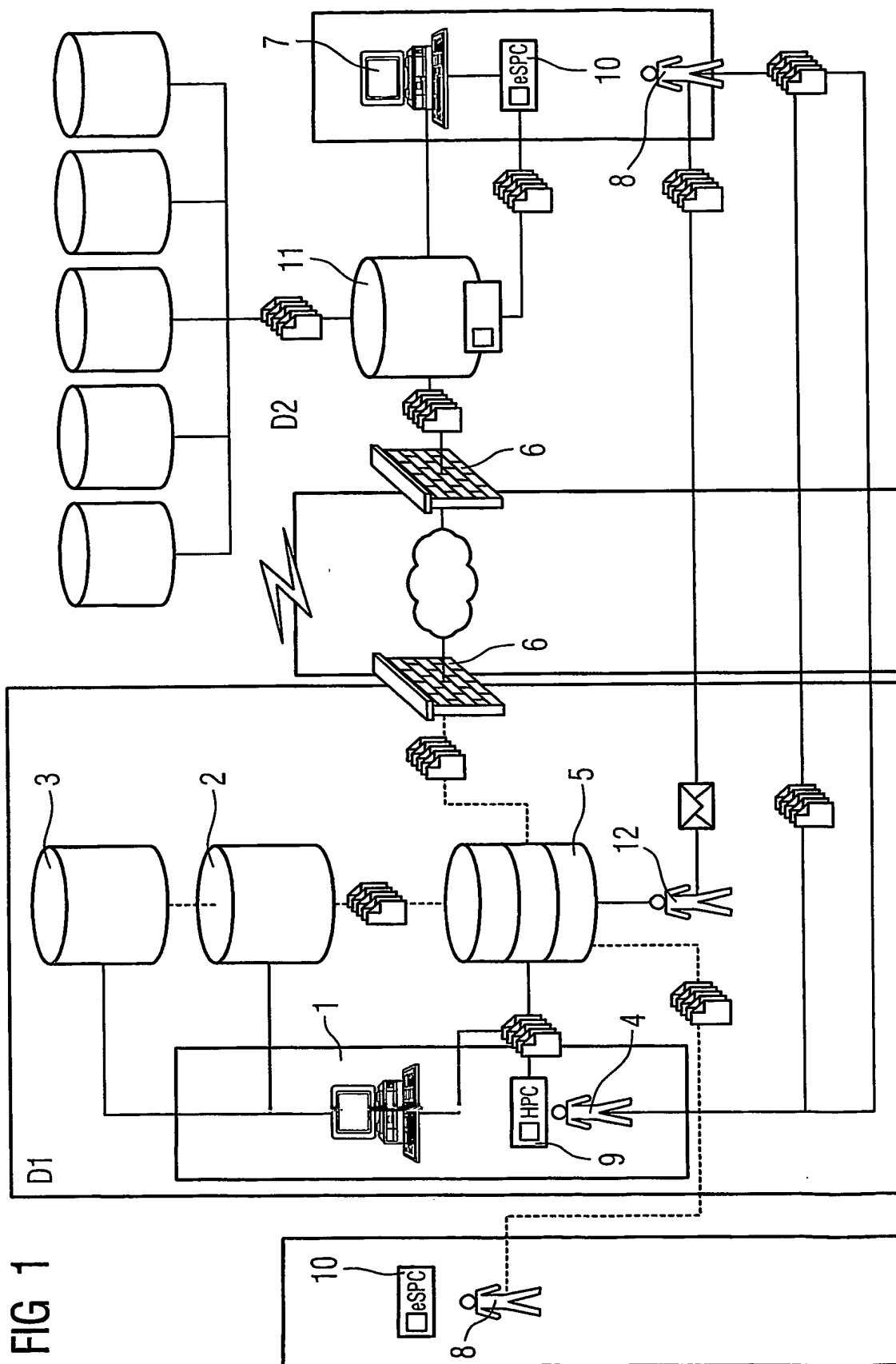


FIG 2

